DWIGHT C. HOLTON, OSB #090540
United States Attorney
District of Oregon
GREGORY R. NYHUS, OSB # 913841
Assistant United States Attorney
1000 S.W. Third Ave., Suite 600
Portland, OR 97204-2902
Telephone: (503) 727-1000
greg.r.nyhus@usdoj.gov
Attorneys for United States of America

UNITED STATES DISTRICT COURT
DISTRICT OF OREGON
PORTLAND DIVISION

UNITED STATES OF AMERICA	**09-CR-321-KI**
v.	**GOVERNMENT'S RESPONSE TO MOTION TO EXCLUDE IMAGES OF THE WU LAPTOP AND EXTERNAL HARD DRIVE**
HOCK CHEE KOO, THONGSOUK SOUTAVONG, et al.,	
Defendants.	

The United States of America, by Dwight C. Holton, United States Attorney for the District of Oregon, through Gregory R. Nyhus, Assistant United States Attorney (AUSA) for the District of Oregon, provides this response to defendant's motion to exclude from evidence forensic images taken from the Wu laptop and external hard drive [1].

Defendant seeks to exclude this digital evidence because he claims the acquisition of the images by the FBI lacks requisite trustworthiness and that the original Wu laptop hard drive lacked evidentiary integrity when images were created from it. Defendant contends that the government failed to obtain and preserve evidence in a manner that preserved its integrity and

[1] Defendant Soutavong moved for a joinder in codefenant Khoo's motions (CR 57).

that the government failed to demonstrate an intact chain of custody.

The government maintains that this digital evidence is admissible under evidentiary standards because the government can properly authenticate the evidence, and that defendant's motion to exclude the evidence is effectively a *Daubert* challenge and, as such, the government need only demonstrate that the underlying seizure of evidence was credible. As such, the government's evidence is admissible and defendant's arguments regarding the quality of the evidence and the nature of its acquisition addresses the weight the fact finder is to assign the evidence.

This Court should deny defendant's motion to exclude the evidence because the manner in which the images were captured adheres to standard forensic guidelines and practices, and that therefore the government can demonstrate proper foundation for and authentication of the evidence. Moreover, evidence being challenged on authenticity grounds should be admitted so long as a reasonable juror could find that evidence to be authentic. Therefore, defendant's arguments are more appropriately directed to the weight the jury should give the evidence, not to the authenticity and/or admissibility of that evidence.

FACTUAL BACKGROUND

Lawrence "Drew" Hoffman owns The Hoffman Group ("THG"), a company that has roughly twenty employees and its principal place of business in Portland, Oregon. THG designs and manufactures products for the after-market automobile industry and distributes these products domestically and internationally. The majority of THG's manufacturing occurs in China., and THG maintains a China office that oversees this manufacturing.

Defendants in this case (Thongsouk Soutavong, Hock Chee Khoo, and Shengbao Wu;

hereinafter, "Soutavong," "Khoo," and "Wu," respectively) are former employees of THG. Soutavong was hired to fill a technical support function and serve as a customer representative; his role was to identify which products were selling well, make recommendations as to how to make adjustments to certain products and serve as a liaison between customers and product developers. Khoo worked in distribution and warehousing. When THG created a new subsidiary company, Marix, Khoo became an employee of this new subsidiary. Wu worked out of the THG office in China, making frequent trips to Portland to consult with Hoffman. Wu's role was to submit product designs to various factories and obtain from the factories price quotations to manufacture the products. Wu's employment with THG was regulated by several agreements, one of which was a non-disclosure agreement.

THG maintained much of its proprietary information regarding product development, processes and factory details in a database that Hoffman believed to be secure. The database held information that THG had an interest in protecting from disclosure to competitors. While certain employees were permitted limited access to the database in order to fulfill their job responsibilities, Hoffman testified that he never gave anyone in THG, including Wu, authorization to download the entire database. On the contrary, Hoffman made efforts to keep the information contained in the database secret.

In August 2006, Hoffman discovered on eBay an auction selling a product that appeared to be identical to one of THG's products, the "130 Degree Lambo Vertical Door Kit." Hoffman researched the domain name of the company offering the product, and determined that the product was being marketed by the company "JES Suppliers, LLC." JES Suppliers had been incorporated in Oregon by THG's former employees Soutavong, Khoo, and Wu. To verify that

the product being sold on eBay was identical to the Lambo Vertical Door Kit produced by THG, Hoffman arranged for a third party to purchase the item through the eBay site. The product was being sold at a lower price than THG's market price for the product. Hoffman received complaints from customers who believed they were being overcharged by THG. Hoffman eventually hired a private investigator, Stephen J. Kahl.[2]

Kahl initiated email correspondence with both Khoo and Wu, portraying himself as a potential business partner. Hoffman testified that Wu sent images to the private investigator of THG products and parts, some of which had not yet been released. Because some of these products and parts were still in development, Hoffman deduced that they would have to have been sent from the THG China office, out of which Wu worked. Hoffman requested a meeting with Wu, and on October 17, 2006, Wu flew to the United States. Hoffman picked up Wu at the Portland airport and brought him to the THG office, where Hoffman introduced Wu to Mark Hansen. Hoffman said that Hansen needed to install an upgrade on Wu's laptop (which was the property of THG). In fact, Hansen was a forensics expert and computer analyst for Northwest Countermeasures. After Wu turned over the laptop, Hansen used Acronis software to make an image of the hard drive onto an external USB hard drive. This image has not been accessed since its creation. Hoffman then took the laptop home, turned it on and examined some of its contents. He attempted to copy the contents of one folder onto a thumb drive, but was unable to do so. On October 20, 2006, Hoffman brought the laptop to the FBI's Northwest Regional Computer Forensic Laboratory, where he met with FBI Special Agent Phil Slinkard.

With SA Slinkard present, Hoffman attached an external USB drive to the computer.

[2] Hoffman also contacted the FBI about this matter, who initiated their own investigation in September 2006.

Hoffman then transferred a copy of a folder on the laptop labeled "Private." SA Slinkard monitored the entire transfer, which took about fifteen minutes. No files were written to the laptop, and once the transfer was complete, Hoffman shut down the computer and turned it over to SA Slinkard. Hoffman also turned over the USB drive containing the image of the laptop obtained by Mark Hansen. SA Slinkard prepared Receipts for Property (FD-597) for both the laptop and the USB drive, and then prepared a Consent to Search (FD-26) for each item. The laptop and the drive were then handed over to FBI Special Agent Joel Brillhart, who created two digital images—one of the USB drive which housed the backup file created by Hansen, and one of the Wu laptop. SA Brillhart used EnCase Forensic Tool Kit software to create these images, and then submitted his work to FBI Special Agent Steve Johns for peer review.

ARGUMENT

I. THE LAPTOP IMAGES AND ACRONIS IMAGES ARE ADMISSIBLE UNDER CURRENT EVIDENTIARY STANDARDS.

Arizona v. Youngblood demands a high bar to exclude evidence that has been obtained by the government: "Unless a criminal defendant can show bad faith on the part of the police, a failure to preserve potentially useful evidence does not constitute a denial of due process of the law." 488 U.S. 51, 58 (1989). Defendant has not demonstrated bad faith or a constitutional violation in the handling and treatment of the evidence he argues should be excluded. Instead, defendant questions the thoroughness of the forensic procedures as to the imaging of the laptop. The forensic procedures that Special Agent Joel Brillhart used, however, adhere to standard FBI protocols. Where forensic examinations are conducted in a "professional and reasonable manner," those examinations are presumed to uphold the integrity of evidence. *Youngblood*, 488 U.S. at 59. Further, law enforcement officials "do not have a constitutional duty to perform any

particular tests." *Youngblood*, 488 U.S. at 59. Therefore, defendant's arguments are more appropriately directed to the weight the jury should give the evidence, not its admissibility.

A. Evidence challenged on authenticity grounds should be admitted so long as a reasonable juror could find that evidence to be authentic.

The trial court determines "whether proffered evidence has enough prima facie trustworthiness to warrant its consideration by the jury." *United States v. King*, 472 F.2d 1, 7 (9th Cir. 1973). Fed. R. Evid. 901(a) provides, "The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." In its notes on Rule 901, the Advisory Committee advises that authentication "represent[s] a special aspect of relevancy," which falls "in the category of relevancy dependent upon fulfillment of a condition of fact and is governed by the procedure set forth in Rule 104(b)." Fed. R. Evid. 104(b) provides, "When the relevancy of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition." Thus, once the sponsor of the evidence makes a prima facie showing of authenticity to the judge, sufficient foundation for that evidence has been laid, and the probative strength of that evidence is a matter for the jury. *United States v. Chu Kong Yin*, 935 F.2d 990, 996 (9th Cir. 1991). The sponsor of the evidence need not prove authenticity beyond a reasonable doubt. *United States v. Logan*, 949 F.2d 1370, 1377-78 (5th Cir. 1991) (internal citations omitted).

This circuit regards challenges to the accuracy and trustworthiness of proffered evidence as relevant considerations to the weight, not the admissibility, of that evidence. *United States v. Catabran*, 836 F.2d 453, 458 (9th Cir. 1988). In *Catabran*, the defendant challenged the

accuracy of computer records evidence on two grounds: accidental data entry error in the creation of the records and unreliability of the computer program that created the records. *Id.* Despite these doubts about evidentiary reliability, "the district court did not abuse its discretion in admitting the [evidence], particularly given the extensive cross-examination on this issue." *Id*. The general rule that trustworthiness concerns are appropriately directed to weight and not admissibility extends to allegations that evidence is tainted because custodians of that evidence have intentionally tampered with it. *United States v. Bonallo*, 858 F.2d, 1427, 1436 (9th Cir. 1988). In *Bonallo*, the defendant argued that records were untrustworthy because they might have been altered by someone who wished to frame him. *Id.* However, merely raising the possibility of tampering, or suggesting that manipulation or alteration of the evidence could have occurred is not sufficient to render evidence inadmissible. *Id.*

Questions about evidentiary reliability that flow from a possible break in the chain of custody also inform the weight, not admissibility, of the evidence. *United States v. Vansant*, 423 F.2d 620, 621 (9th Cir.), *cert. denied*, 400 U.S. 835 (1970); *United States v. Godoy*, 528 F.2d 281, 284 (9th Cir.1975). The district court may admit the evidence if there is a "reasonable probability the article has not been changed in important respects." *Gallego v. United States*, 276 F.2d 914, 917 (9th Cir 1960). Moreover, where no evidence indicating otherwise is produced, "the presumption of regularity supports the official acts of public officers, and courts presume that they have properly discharged their official duties." *Id.* See also, *United States v. Harrington*, 923 F.2d 1371, 1374 (9th Cir. 1991).

///

///

B. The government can adequately authenticate the data in the laptop image and the Acronis image by demonstrating that standard forensic procedures were applied to the acquisition and handling of the evidence.

Defendant suggests two bases for the exclusion of the images—that the circumstances in which the images were obtained compromise the authenticity of the evidence, and that the integrity of the original Wu laptop was jeopardized after Wu relinquished control of it. However, neither of these challenges merit altogether exclusion of the evidence.

Defendant argues that the laptop image and Acronis image were acquired in a manner that departed from standard forensic procedures. Defendant offers a declaration from computer expert Michael Bean, which advances a description of what "proper authentication" by the FBI would have entailed, and states how the procedures actually used depart from Bean's conception of "proper authentication." (Declaration of Forensic Computer Expert Bean, at pp. 7-8). Defendant concedes that "it is difficult to assess the ultimate impact of these deviations from recognized forensic computer examination protocol," yet still maintains "there is no doubt that these deviations from accepted practice seriously undermine confidence in the validity of the Wu Laptop and Acronis images." (Def's Mot to Excl, p. 19)[3]. Defendant makes this concession even though no material or documentation regarding the extraction protocols were provided to defendant. Thus, defendant is unable to identify harm that flows from the protocol that was used. Similarly, defendant points to "unexplained dating discrepancies" as evidence of unreliability of the evidence. *Id.* The images produced by the FBI, defendant argues, bear creation dates that predate the FBI's actual possession of the Acronis image and the laptop itself.

[3] The government interprets defendant's challenge to authenticity of the forensic protocols themselves as a *Daubert* motion, and responds to this in section II, infra.

Id. However, defendant also allows that these "unexplained dating discrepancies" might very well be "attributable to simple carelessness." *Id.* at 20.

Any facial inaccuracies of the evidence that exist, however, go "to the weight of the evidence, not its admissibility." *Catabran*, 836 F.2d at 458. In *Catabran*, where both human and computer error produced inaccuracies apparent in the evidence, the magnitude of those inaccuracies was properly explored through witness testimony and cross-examination. *Id.* Here, as in *Catabran*, if there is any import to inaccuracies such as "unexplained dating discrepancies," it is to be determined by the jury.

Defendant also suggests that the Wu's relinquishment of his laptop to Hansen resulted in a tainted chain of custody requiring heightened scrutiny. However, merely raising the possibility of tampering is not sufficient to render evidence inadmissible. *United States v. Harrington*, 923 F.2d 1371, 1374 (9th Cir. 1991) (internal citation omitted). Evidence rebutting the assertion is something given to the weight, not the sufficiency, of the evidence.

Defendant directs the court to the Seventh Circuit case, *United States v. Jackson*, as an analogous examination of authentication concerns. (Def's Mot to Excl, p. 15). However, the aggravated facts and ensuing reasoning of Jackson do little to inform this case. In *Jackson*, the defendant was convicted of mail fraud, wire fraud, and obstruction of justice for attempting to smear a mail delivery service by sending racist hate mail under its logo. 208 F.3d 633, 634-36 (7th Cir. 2000). Jackson appealed her conviction, and argued that the trial court abused its discretion when it did not allow Jackson to bring in evidence of website postings allegedly made by white supremacist groups, which apparently took credit for Jackson's racist mailings and would therefore have exonerated her. Id. at 637. In addition to listing a host of reasons why the

website postings were properly excluded (that they were hearsay, unfairly prejudicial, and irrelevant; that "any evidence procured off the Internet is adequate for almost nothing" (internal citation omitted)), the *Jackson* court also found the website postings lacked authentication under Fed. R. Evid. 901 because the defendant offered no proof that the postings were in fact made by the supremacist groups. *Id.* at 638.

The evidence in *Jackson* was properly excluded not because it was "of a type that is easily open to alteration or manipulation, and the circumstances disclose[d] a suspicious chain of custody and the possibility of data manipulation," as defendant suggests (Def's Mot to Excl, p. 16). Rather, the evidence was properly excluded because the sponsor of the evidence made no prima facie showing of authenticity whatsoever. 208 F.3d at 638. Further, while the court in *Jackson* ultimately deemed the web posting evidence inadmissible, it also noted that the government's initial challenge to the evidence—that it was fabricated—was deficient. An opponent to a piece of evidence cannot adequately challenge that evidence on authenticity grounds simply by "pronounc[ing] it phony." *Id.* at 637. On the contrary, "[s]orting truth from fiction . . . is for the jury." *Id.*

Here, the government can authenticate the laptop image and the Acronis image because the FBI employed standard forensic procedures upon taking possession of the evidence. Special Agent Joel Brillhart used EnCase software to duplicate the data, and his work was then peer-reviewed by another examiner at the Regional Computer Forensics Lab (RCFL), which was checked for the proper protocols and accuracy. If defendant has challenges to raise regarding these standard forensic procedures that were used, then those challenges are more appropriately addressed in a *Daubert* motion, which is discussed below.

II. A CHALLENGE TO THE SUFFICIENCY OF FORENSIC STANDARDS SHOULD BE TREATED AS A *DAUBERT* CHALLENGE AND ANALYZED ACCORDINGLY.

A. Evidence that meets the *Daubert* standards for relevance and reliability should be admitted so as to help the jury evaluate the case.

Federal Rule of Evidence 702 allows admission of "scientific, technical, or other specialized knowledge" by a qualified expert if it will "assist the trier of fact to understand the evidence or to determine a fact in issue." In determining if evidence should be admitted under Rule 702, courts should conduct a "flexible" inquiry. *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 594 (1993); see also *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 147 (1999) (extending "gatekeeping" function of a district court to matters of all expert testimony). When the reliability of evidence is at issue, "[v]igorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence." *Daubert* 509 U.S. at 596. Further, "[i]f two contradictory expert witnesses [can offer testimony that is reliable and helpful], both are admissible" and the credibility of those contrary experts is a matter not for the court, but for the fact-finder. *Dorn v. Burlington N. Santa Fe R.R. Co.*, 397 F.3d 1183 (9th Cir.2005) (internal citation omitted).

As a threshold matter, admitted evidence must be relevant, meaning it will assist the trier of fact to understand or determine a fact in issue. *Daubert*, 509 U.S. at 591-92. The second prong of the *Daubert* test requires that evidence be reliable to be admissible. However, "[a] trial court not only has broad latitude in determining whether an expert's testimony is reliable, but also in deciding how to determine the testimony's reliability." *Mukhtar v. California State Univ.*,

299 F.3d 1053, 1064 (9th Cir. 2002); see also *United States v. Hankey*, 203 F.3d 1160, 1168 (9th Cir.2000). While the trial court should "exclude 'junk science,'" *Mukhtar* 299 F.3d at 1063, *Daubert* provides an otherwise flexible guide for the trial court as to how to assess the reliability of expert evidence. *Daubert*, 509 U.S. at 593-94. Factors a trial court may, but not must, consider to guide a reliability assessment include: (1) whether a scientific theory or technique can be (and has been) tested; (2) whether the theory or technique has been subjected to peer review or publication; (3) the known or potential rate of error and the existence and maintenance of standards controlling the technique's operation; and (4) whether the technique is generally accepted. *Id.* Such "factors [were] meant to be helpful, not definitive. Indeed, [these] factors do not all necessarily apply even in every instance in which the reliability of scientific testimony is challenged." *Kumho*, 526 U.S. at 151.

B. The forensic methods used to acquire the laptop image and Acronis image substantiate the admissibility of the digital evidence.

The party who presents an expert must demonstrate that the expert's findings are based on sound principles and that they are capable of independent validation. *Daubert*, at 1316. Here, the government intends to make the requisite showing of reliability for the methods that were used to obtain and duplicate the images of the laptop and external hard drive.

Special Agents Phil Slinkard and Joel Brillhart complied with forensic protocols that are standard for the FBI's acquisition of evidence. Brillhart used EnCase software to create an exact image of the Wu laptop. Brillhart then submitted his work to another examiner for peer review. Evidence will be presented as to the reliability of the procedures used, as well as SA Brillhart's treatment of this digital evidence in particular. The government will also offer testimony that

establishes that the techniques used in this case conformed with the methodologies typically employed by the FBI in the collection of digital evidence. That defendant wishes to counter this testimony with an expert who will challenge the validity of these standard FBI protocols in no way merits the exclusion of the digital evidence that the government proffers. Instead, it is a matter for the jury to determine the credibility of the competing expert witnesses.

CONCLUSION

Exclusion of evidence is an extraordinary remedy limited to instances where a defendant cannot demonstrate bad faith on the part of law enforcement agents who obtained the evidence and is usually reserved for constitutional violations. The matters that defendant raises in regard to the digital evidence are relevant to the weight of that evidence, not its admissibility. Defendant's motion should be denied.

DATED this 12th day of October 2010.

Respectfully submitted,

DWIGHT C. HOLTON
United States Attorney
District of Oregon

s/ Gregory R. Nyhus

GREGORY R. NYHUS, OSB #913841
Assistant United States Attorney